BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch submission to the Science and Technology Committee on the inquiry into the work of the Biometrics Commissioner and the Forensic Science Regulator

May 2019

About Big Brother Watch

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

Introduction

We welcome the opportunity to submit evidence to the inquiry into the work of the Biometrics Commissioner and the Forensic Science Regulator.

This submission will focus on the continued retention of innocent people's custody images on police databases and the police's use of biometric live facial recognition cameras.

We call on the Government to:

- **Immediately end UK police use of live facial recognition in public spaces in order to prevent unnecessary and disproportionate infringements of the fundamental rights to privacy and freedom of expression and association, unlawful police action and potential discrimination;**
- **Immediately introduce a policy of automatic deletion of the custody images of unconvicted individuals from police databases, and remove all historic images of unconvicted individuals;**

1. Custody Images

1.1 The continued retention of hundreds of thousands of innocent people's custody images on the Police National Database,[1] the increasing number of images held, and their creation into searchable facial biometric images for use within live facial recognition watchlists, is a source of serious concern.

1.2 The High Court ruled in 2012 in *RMC & FJ* that the indefinite retention of innocent people's custody images was "unlawful",[2] but neither the Home Office nor the police have taken any action to resolve this.

The custody image review: a failed response

1.3 In a response that took 5 years, the Home Office created a policy in their 2017 Custody Image Review whereby innocent people could write to their local police force to request the deletion of their custody image.[3] However, the new policy doesn't meet the minimum requirements set out in the 2012 judgment and it has been exposed as a failure.

1.4 A Press Association investigation revealed only 67 applications for deletion had been made, and only 34 had been successful.[4] The Biometrics Commissioner confirmed in his evidence to the Science and Technology Committee that the Home Office has done nothing to promote this review and that people needed to "*google it and find it out for themselves*".[5] The Information Commissioner has also said:

> "*it is unclear how those individuals would know that they could make a request and we are aware that there have not been a significant number of requests, indicating a lack of awareness*".[6]

1 BBC News Online, 'Facial recognition database 'risks targeting innocent people', 14 September 2018 (http://www.bbc.co.uk/news/uk-41262064)

2 *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)

3 Home Office, 'Review of the Use and Retention of Custody Images', February 2017 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf)

4 Press Association: 'Custody image' deletion request figures, 12 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.htm)

5 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

6 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

1.5 The Biometrics Commissioner said in his evidence to the Science and Technology Committee that at the time the Custody Image Review was published, he "*was not at all sure [the Review] would meet further court challenges*" and that he still believes this is the case: "*I am not sure that the legal case is strong enough and that it would withstand a further court challenge*".[7]

1.6 The Information Commissioner has also said that "*there are potentially thousands of custody images being held with no clear basis in law or justification for the ongoing retention*".[8]

1.7 The previous Biometrics Commissioner estimated that hundreds of thousands of custody images on the Police National Database are of innocent people – people who were not charged, or who were found not guilty.[9]

One of the largest biometric databases in the UK

1.8 The Biometrics Commissioner updated the Science and Technology Committee on the number of custody images currently held on the Police National Database – 23 million. This is an increase of 4 million since the previous figures were updated just one year ago.[10] According to the Biometrics Commissioner, a staggering 10 million of these images have now been made biometrically searchable by facial recognition technology,[11] following an upgrade to the system in 2014 which occurred without parliamentary or public scrutiny.[12]

1.9 With sub-sets of this database being used at police deployments of live facial recognition, innocent people are increasingly at risk of being wrongfully stopped or even arrested. This also completely blurs the line between the innocent and the guilty, and makes a mockery of the presumption of innocence.

7 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

8 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

9 BBC News Online, 'Facial recognition database 'risks targeting innocent people', 14 September 2018 (http://www.bbc.co.uk/news/uk-41262064)

10 Press Association: 'Custody image' deletion request figures revealed, 12 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.htm)

11 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

12 Science and Technology Committee: Oral Evidence – Biometrics Strategy and Forensic Services, 6 February 2018. (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/biometrics-strategy-and-forensic-services/oral/78113.htm)

1.10 The Home Office has claimed that there would be prohibitive costs involved in deleting innocent peoples images.[13] However, at the same time, the Home Office has awarded millions in funding to police to implement automated facial recognition – including £2.6million to South Wales Police.[14]

1.11 We understand there is currently an ongoing discussion within the Home Office as part of the new Law Enforcement Database Service, which is the planned upgrade to policing systems, about how historic images of unconvicted people can be deleted. However, Baroness Williams would not even commit to a date for this removal when pressed by the Committee - although it is now 7 years since the 2012 High Court ruling.[15]

1.12 **We call on the Home Office to immediately remove all historic images of unconvicted people from the custody image database, and to introduce a policy of automatic deletion of the custody images of unconvicted individuals from police databases, in line with legal requirements.**

13 The Independent, ''Too expensive' to delete millions of police mugshots of innocent people, minister claims' 19 April 2018 (https://www.independent.co.uk/news/uk/politics/police-mugshots-innocent-people-cant-delete-expensive-mp-committee-high-court-ruling-a8310896.html)

14 South Wales Police and Crime Commissioner, Medium Term Financial Strategy2017-2021 (https://pcclivewww.blob.core.windows.net/wordpress-uploads/2016-12-28-Final-Medium-Term-Financial-Strategy.pdf)

15 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

2. Police use of live facial recognition in public spaces

2.1 There are significant concerns over the legality of the police's use of live facial recognition, particularly the likely infringement of people's fundamental rights, the aggressive over-policing witnessed during deployments, its use for non-criminal purposes, as well as the spurious nature of the police's 'trial'.

2.2 We have revealed that the police's use of live facial recognition has been over 90% inaccurate, following freedom of information requests to the police, and this staggering inaccuracy rate has continued throughout the police's use of the technology.[16]

2.3 There is also a significant risk of racial and gender bias of the technology, with the the Metropolitan Police Senior Technologist admitting that they had found significant gender bias in their technology.[17]

2.4 Despite this, the police have continued to deploy live facial recognition in public spaces, indiscriminately scanning innocent members of the public and consistently misidentifying them as wanted criminals.

No legal basis

2.5 There is no legal basis for the police's use of live facial recognition surveillance. This has been said many times before, but in light of Baroness William's incorrect claim to the Science and Technology Committee that "*there is already a legal framework for the use of LFR*",[18] it bears repeating.

2.6 When Layla Moran MP posed a written question to the Home Office about current legislation regulating "*the use of CCTV cameras with facial recognition and biometric tracking capabilities*", Nick Hurd MP (Minister for Policing, responding for the Home Office) answered: "*There is no legislation regulating the use of CCTV*

16 https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf; https://bigbrotherwatch.org.uk/all-media/campaigners-urge-met-to-drop-disastrous-facial-recognition/

17 https://www.ucl.ac.uk/jill-dando-institute/events/2019/may/just-looking-learning-police-trials-live-facial-recognition

18 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/98672.pdf

cameras with facial recognition".[19] The Metropolitan Police have also acknowledged that "*There is currently no specific legal framework in the use of this technology*."[20]

2.7 The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras in England and Wales. There is no reference to facial recognition in the Protection of Freedoms Act, although it provides the statutory basis for public space surveillance cameras.

2.8 Police have claimed that their use of live facial recognition is regulated by the Protection of Freedoms Act 2012 and the Data Protection Act 2018. As with the Protection of Freedoms Act 2012, there is not a single mention of live facial recognition in the Data Protection Act 2018. The Surveillance Camera Commissioner said in recent evidence to the Science and Technology Committee that:

> "*The Data Protection Act 2018 alone does not provide a basis in law for use of this technology nor does the completion of a Data Protection Impact Assessment* (DPIA)."[21]

2.9 Meanwhile, the Biometrics Commissioner stated that "*PoFA* [Protection of Freedoms Act] *is not generic legislation covering all biometrics used by the police*" and therefore that "*the use by the police of these second generation biometrics is not currently governed by any specific legislation.*"[22] He added that for "*each use of biometric information the balance between public benefit and individual privacy (proportionality) should be decided by Parliament.*"[23]

Over-policing during deployments

2.10 We are seriously concerned by several recent incidents that occurred during live facial recognition 'trial' deployments by the Metropolitan Police in London. In our observations of these 'trial' deployments, we witnessed people being stopped for merely covering their faces, and one extremely concerning incident

19 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/
20 https://www.london.gov.uk/press-releases/mayoral/independent-panel-delivers-report-on-polices-use
21Surveillance Camera Commissioner evidence to the Science and Technology Committee, March 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97777.html
22Biometrics Commissioner, Annual Report 2017 (June 2018)
23Biometrics Commissioner, Annual Report 2017 (June 2018)

where a child in school uniform was stopped, surrounded by plainclothes police, and fingerprinted following a system misidentification.

2.11 We have documented several case studies, below:

Case study 1 – February 2019

A 14 year old black school child, wearing school uniform, was wrongly identified by the facial recognition system, and subsequently surrounded by four plainclothes police officers. He was pulled onto a side-street, his arms held, questioned, asked for his phone, and even fingerprinted. He was released after ten minutes when police realised they had the wrong person. The child appeared frightened and said he felt was being harassed by police.

Case study 2 – January 2019

A man was stopped for covering his mouth and chin with his jacket after seeing facial recognition signs and expressing his objection to the deployment. His reaction was observed by a plainclothes police officer who followed him and radioed through to other officers to make a stop. Police demanded his ID and the man complied. However, protesting against the facial recognition cameras, he was issued with a £90 public order fine for 'shouting profanities in public view'. The man was not wanted for any crime, and after being fined, he was released.

Case study 3 – December 2018

A young man was stopped by two police officers for covering his mouth and chin with his scarf as he walked past a police live facial recognition van. He was trying to keep warm on a freezing cold day. The two police officers asked for his details and checked his ID against the police database, letting him go after he didn't come up as wanted. He was distressed at having been stopped and made late for work. He was not aware of the live facial recognition surveillance or what it was.

Case study 4 – January 2019

On the coldest day of the year, a young black boy in school uniform, wearing a hooded jacket, was stopped and forced to show his ID as he was not visible to the facial recognition cameras. His friend told us he was distressed and had felt harassed.

Use for non-criminal purposes

2.12 The police have used live facial recognition to identify and monitor people who aren't wanted for any crime. At Remembrance Sunday in November 2017, the Metropolitan Police used live facial recognition in attempt to identify a dataset of 'fixated individuals' – a loosely defined watchlist of people who are alleged to frequently contact public figures and who are highly likely to suffer mental health issues, but who were not suspected of or wanted for any criminal activity.

2.13 This non-criminal application of facial recognition technology resulted in a so-called 'fixated individual' being identified and subsequently ejected from the ceremony by police. The use of this authoritarian technology to target people suffering mental ill health is an unprecedented infringement of civil liberties and could have serious adverse health effects.

2.14 This also has very serious implications for the ongoing criminalisation and stigmatisation of people who are unconvicted or not currently wanted for any crimes. If the police are allowed to target vulnerable individuals for non-criminal purposes, there is nothing to stop them identifying and tracking any of the hundreds of thousands of unconvicted people who they hold custody images for, or indeed other image sources.

Future use of live facial recognition

2.15 The Biometric Strategy did not provide any updated guidance or safeguards in relation to police use of live facial recognition. The Biometrics Commissioner said it was merely "a list of some of, but by no means all, the things that the Home Office is doing on the use of biometrics" and that it was "confusing and disappointing" and a "missed opportunity".[24]

2.16 While there is no commissioner who has oversight over the police's use of live facial recognition, all of the relevant commissioners – the Biometrics Commissioner, the Information Commissioner, and the Surveillance Camera Commissioner – have been heavily critical of its use.

24 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

2.17 Baroness Williams told the Committee that the police "*have also been to the modalities board — the face and new biometrics oversight board — before they deploy the technology in live facial recognition trials.*"[25] However, this Board was only created in July 2018, almost two years after the police began using live facial recognition in August 2016.

2.18 The Biometrics Commissioner made his view on the police's continued use of live facial recognition clear to the Committee in March 2019, stating:

> *"[T]his would not be a sensible time to start routinely to deploy AFR [live facial recognition] operationally; a number of questions still need to be answered."*

2.19 He also said that any future decision on whether police can use live facial recognition is extremely important and therefore has to be made by Parliament:

> *"Given the public importance of that proportionality decision and the fact that things like automatic facial recognition systems will potentially affect the life of every citizen, because this is mass surveillance through facial imaging, it seems to me that it is very much in the public interest that that decision should be taken in a public way. I would have thought that the obvious body to do that was yourselves — Parliament."*[26]

2.20 Meanwhile the Information Commissioner has said that she is:

> *"so concerned with the practices in some areas that a priority investigation has been opened to understand and investigate the use of AFR by law enforcement bodies in public spaces."*[27]

2.21 The Information Commissioner has said that the Science and Technology Committee's "*current concerns over the technology's effectiveness and potential*

25 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)
26 Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)
27 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

bias" have "*not been fully addressed and it is not yet clear how the 'oversight board' will address these issues.*"[28]

2.22 The Commissioner has also expressed concern about "*the more general roll out of AFR and whether they have been able to demonstrate full compliance with the DPA18* [Data Protection Act 2018]."

Race and gender bias

2.23 There are serious concerns about the discriminatory impact of live facial recognition surveillance. A number of independent studies have found that various facial recognition algorithms have demographic accuracy biases – that is that they misidentify some demographic groups, particularly women and people of colour, at higher rates than others, such as white men. A study found that commercial facial recognition technologies, including those created and sold by Microsoft and IBM, had error rates of up to 35% when identifying the gender of dark-skinned women compared to 1% for light-skinned men (Buolamwini & Gebru, 2018).[29] A follow up study found that Amazon's 'Rekognition' software mistook women for men 19% of the time, and darker-skinned women 31% of the time (Raji & Buolamwini, 2019).[30]

2.24 The Biometrics and Forensics Ethics Group warned that UK police's use of live facial recognition technology has the "*potential for biased outputs and biased decision-making on the part of system operators*".[31]

2.25 The Metropolitan Police has been aware of these concerns since 2014, when it was raised during an Association of Chief Police Officers (ACPO) 'Facial Imaging Working Group'.[32] We have asked the police on several occasions whether they would carry out or commission demographic accuracy bias testing, and they told us that they would not because they did not view it as an issue.

2.26 However, in the Metropolitan Police's written evidence to the Science and Technology Committee, the force has now admitted there are issues:

28 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf
29 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
30 http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf
31 Biometrics and Forensics Ethics Group, Interim report, February 2019
32 Obtained through Freedom of Information Requests.

> "*The MPS is cognisant of the concern over the system response with respect to different demographics. We are working to further mitigate potential impact of this within the operational context, where it should be noted, additional checks and balances are in place and the final decision is by a human operator."*[33]

2.27 This suggests the police has noticed the need to "mitigate" the discriminatory impact, despite the fact that this has never been formally tested by them. They also claim that a human review of a match prior to stopping someone can mitigate the risk of ethnic minorities disproportionately being matched and misidentified, which is plainly an untrue and unacceptable position. They continued, "*The MPS plans to continue to test demographic differences"* - a long overdue and confusing commitment, given that MPS has never before tested demographic differences and has thus far resisted all of our calls to do so.

2.28 In a presentation at University College London on 29 May 2019 about their use of live facial recognition, the Metropolitan Police Senior Technologist, Johanna Morley, admitted that they had found significant gender bias in their technology – that it misidentified women at higher rates that men.[34]

2.29 However, its important to note that our analysis and the analysis of many human rights groups around the world is that even if live facial recognition technology improves in demographic and general accuracy it remains too great a risk to civil liberties, dangerously imbalances power between citizen and state, and constitutes a fundamental threat to the right to privacy.

Right to privacy and freedom of expression and association

2.30 We are currently bringing a legal challenge against the Metropolitan Police and the Home Secretary regarding the use of live facial recognition in public spaces. We have received expert legal advice that the police's use of this technology is likely to breach people's right to privacy, and their freedom of expression and association.

33 Written evidence submitted by Metropolitan Police Service (WBC0005), 19 March 2019: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97851.pdf

34 https://www.ucl.ac.uk/jill-dando-institute/events/2019/may/just-looking-learning-police-trials-live-facial-recognition

2.31 The Human Rights Act 1998 requires that any interference with the Article 8 right to a private life is both necessary and proportionate. However, the use of live facial recognition with CCTV cameras in public spaces appears to fail both of these tests.

2.32 Live facial recognition cameras scan the faces of every person that walks within the view of the camera; the system creates, even if transitorily, a biometric scan of every viewable person's face; it compares those biometric scans to a database of images; and it retains photos of all individuals 'matched' by the system, despite 96% of matches inaccurately identifying innocent people. It gives the police the ability to track people across public and civic spaces.

2.33 It is plainly disproportionate to deploy a public surveillance technology by which the face of every passer-by is analysed, mapped and their identity checked. Furthermore, a facial recognition match can result in an individual being stopped in the street by the police and asked to prove their identity and thus their innocence.

2.34 Members of the public who have been scanned by live facial recognition are unlikely to be aware that they were subject to the identity check, and do not have a choice to consent to its use. The Biometrics Commissioner commented:"(*...)unlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge.*"[35]

2.35 The Surveillance Camera Commissioner has said that "*overt use of such advancing technology (AFR) [live facial recognition] is arguably more invasive than some covert surveillance techniques*."

2.36 The right to freedom of expression and association – the right to go about your daily activity undisturbed by state authorities, to go where you want and with whom, and to attend events, festivals and demonstrations – is a core principle of a democratic society protected by Article 10 of the Human Rights Act 1998.

2.37 The use of live facial recognition with CCTV has a chilling effect on people's attendance of public spaces and events, and therefore their ability to express ideas and opinions and communicate with others in those spaces.

2.38 **We call on the Government to Immediately end UK police use of live facial recognition in public spaces in order to prevent unnecessary and**

35 Biometric Commissioner, *Annual Report 2016*, September 2017, para. 305

disproportionate infringements of the fundamental rights to privacy and freedom of expression and association, unlawful police action and potential discrimination.

Griff Ferris

Legal and Policy Officer, Big Brother Watch

May 2019